Posudek vedoucího bakalářské práce

Název: Krychlové útoky
Autor: Josef Bárta

Shrnutí obsahu práce

Práce se zabývá krychlovými útoky a jejich rozšířeními. Tyto útoky byly představeny v článku [3] od I. Dinur a A. Shamir a student je popisuje v úvodu kapitoly dva jako C-linearizaci. Zbytek práce obsahuje vlastní příspěvky studenta. Ty začínají navrženými jednoduchými technikami T-linearizace a spojením obou přístupů do TC-linearizace. Třetí kapitola popisuje proudovou šifru Trivium a její zjednodušení pro účely testování efektivnosti navržených technik. To je popsáno ve druhé polovině kapitoly tři.

Celkové hodnocení práce

Téma práce. Téma a náročnost práce jsou přiměřené pro bakalářskou práci. Zadání bylo splněno.

Vlastní příspěvek. Vlastním příspěvkem studenta je hlavně rozšíření původního krychlového útoku využívajícího C-linearizace na útoky pomocí TC-linearizace. Student dále tyto techniky naimplementoval a otestoval na zjednodušené šifře Trivium. V neposlední řadě student rigorózně popsal podstatu původních krychlových útoků.

Matematická úroveň. Velmi dobrá.

Práce se zdroji. Všechny zdroje jsou správně citovány.

Formální úprava. Výborná.

Závěr

Práci považuji za vynikající a doporučuji ji uznat jako bakalářskou práci.

Michal Hojsík
Katedra algebry
10.8.2014